

Current & Future Cyber Threats

Hackers, Criminals & Terrorists

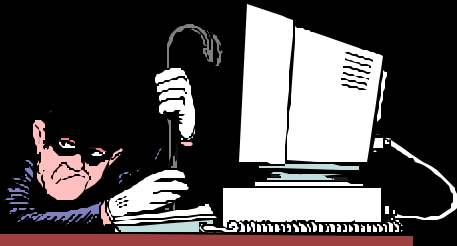
New York Oracle User's Group (NYOUG)

Jan. 10, 2002

Dan Verton

Senior Writer, Computerworld

dan_verton@computerworld.com



Topics of Discussion

- Hackers, Criminals & Terrorists
 - ◆ Who are they?
 - ◆ Motivations?
 - ◆ Tactics?
- Defenses?
- Future?



Hackers



■ Who Are They?

- ◆ Historically good guys, techies
- ◆ White hats, black hats, gray hats, script kiddies, crackers, foreign intelligence, competitors, former employees, hacktivists
- ◆ Predominantly male
- ◆ Ages 13 to 30
- ◆ Middle to upper class economically
- ◆ Diverse geography, ethnicity, education
- ◆ Smart, look like everybody else, act like everybody else, work and live among us

Example 1



MICROSOFT OWNED!

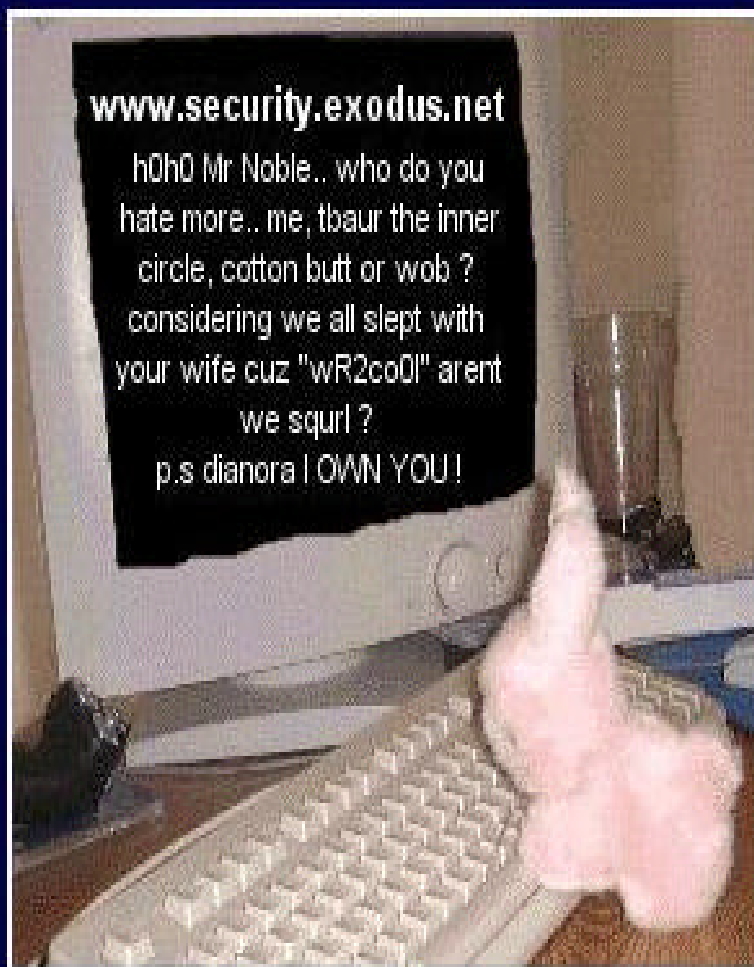
where is the security?

now a company was the time of microsoft.com
who manufactures servers says IIS
windows 2000 + IIS5 one mixes perfect as voceis they
can see!

the true Brazilian groups are Prime Suspectz,
Izc0rp, Crime boys and Supreme Entity
the others in them only burn each time more for
being Brazilian.

Example 2

www.security.exodus.net



FREE THE SHADOW KNIGHT

Fluffi Bunni OWNZ YOU.

Ongoing analysis of your networks vulnerabilities will allow the hackers who own our network to simply read the logs of what is vulnerable on your system and dot slash hack them without even having to scan you. With this service, you are gaurateed to be hacked because if the dot slash hacking fails, we have left a failsafe system which allows any idiot to use one of our scripts to connect to your secure machines using our password by typing a simple command(`s0 goto ip`)"

How Different Are They?



How Different Are They?

SOLD

Bord du lac project

Ile Bizard
Place des Cageux
Model home 303 du Golf St.

Sale price: \$ 314,000.00

Lot #: 184.440

Land of : 11, 376 sq ft


Backyard on Golf

Included: Municipal services (100%) G.S.T. & P.S.T.



Le Montrachet 2000



 Internet

Hackers

■ Motivations

- ◆ Curious about technology, enjoy the rush, challenge
- ◆ Strong opinions about regulation and information ownership
- ◆ Strong sense of political and social responsibility (hacktivism)
- ◆ Look at hacking as a public service (Web site defacement)
- ◆ Increasingly angry, disconnected, anti-government, anti-establishment, violent
- ◆ Shock value

Groups

[Hi-Tech Hate]

Net-Mafia

Silver Lords

Crime Lordz

Prime Suspectz

Cr1m3 Org4n1z4d

Hackers

Stats

1999: 9,000 incidents
2000: >21,000

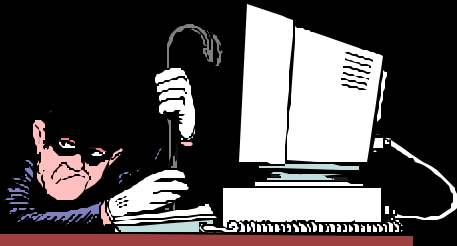
2000: 800 vuln. Reports
2001: >3,000

Microsoft

2000: 100 bulletins
2001: >42 (Aug.)

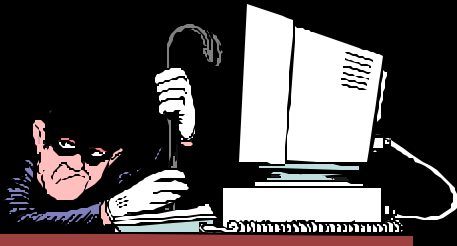
■ Tactics

- ◆ Look & listen for new vulnerabilities, exploits
- ◆ Massive scans for vulnerable machines, reconnaissance, zombies
- ◆ Automated tools, scripts, worms
- ◆ Target Web applications
- ◆ They know YOU don't install every patch
- ◆ Scripts, tools developed within 1-2 weeks of vulnerability



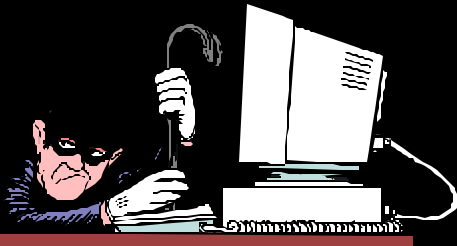
Criminals

- Who are they?
 - ◆ Black hats, crackers, groups, individuals, disgruntled employees
 - ◆ Tend to be older
 - ◆ More sophisticated: they know what they are doing is illegal
 - ◆ Want to enter network undetected and leave without a trace
 - ◆ Diverse geography: Russia primary source of a toxic blend of crime, business & politics



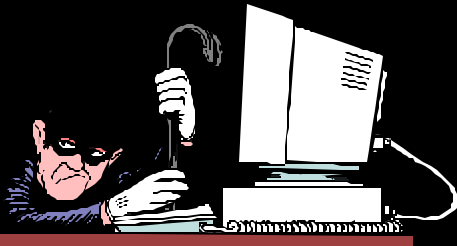
Criminals

- Motivations?
 - ◆ Fraud, theft, extortion
 - ◆ Vandalism, destruction, denial of service
 - ◆ Don't want the attention (i.e. defacements)
 - ◆ Espionage for sale
 - ◆ Revenge: lay-offs, denied promotions, feelings of being misused by management
 - ◆ Feel powerless: at work & in their lives
 - ◆ Little fear of being caught



Example – Cybercrime Tactics

- Internet Trading Technologies Inc.
 - ◆ Jan. 2000, corporate expansion underway
 - ◆ Two software developers approach COO and demand money
 - ◆ Increased demands, threatened to allow development work to founder
 - ◆ First DOS hit on a Thursday morning
 - ★ Crashed app server
 - ★ Attacks continue through weekend
 - ◆ Going out of business was a real possibility



Example 2 – Cybercrime Tactics

- Major bank in Northeast
 - ◆ Feb. 2001 discovered unauthorized purchases being made using customer accounts
 - ◆ Called in security firm, which conducted 131 hours of forensics
 - ◆ Convinced they had an insider helping the hacker
 - ◆ Contractor in Europe had stolen passwords from his mother who was an employee of the bank



Cybercrime Statistics

- FBI/CSI Survey 2000
 - ◆ Total **reported** losses (1997-2000): \$626,586,240
 - ◆ (2000)
 - ◆ Theft of proprietary data: \$66,708,000
 - ◆ Financial fraud: \$55,996,000
 - ◆ Insider abuse: \$22,554,500
 - ◆ Sources of attack
 - ◆ 81% said disgruntled employees
 - ◆ 77% said outside hackers
 - ◆ 44% said competitors



Terrorists & Cyberterrorism

- As of Sept. 11, 2001
 - ◆ ALL BETS ARE OFF
 - ◆ Textbooks are being re-written
- Facts still remain
 - ◆ Businesses are targets
 - ◆ Tactics more violent & deadly
 - ◆ Technology assisting command, control, communications, intelligence
 - ◆ Maybe Bin Laden's grandchildren will attempt cyberterrorism

Defenses

- Download & apply ALL patches when made available
- Get policies, restrict access (physical & electronic)
- Review logs, get a cyber alarm system, emergency action plans
- Audit yourself
- Use hardened system configurations, isolate Web server/public networks from internal network, backup Web content on secure host, use multiple levels of defenses & authentication schemes
- Find the local InfraGard chapter and join it and report intrusions

Future

- Worms, bad code, zombies
- Wireless
 - Most companies don't know they have unauthorized wireless access points leading into their networks
 - WEP is cracked; new standard coming
 - 80% of companies that do use wireless don't turn on encryption
 - If you want to use wireless, learn how to use VPNs